16 STRON EKSTRA

PRZEJĘCIA KONT, CI: RADZIMY, JAK WALCZYĆ!

▸ JAK REAGOWAĆ NA HEJT W SIECI ▸ JAK PRAWO I POLICJA MOGĄ NAM POMÓC ▸ JAK ZBIERAĆ DOWODY NĘKANIA ▸ CO GROZI ZA STALKING ▸ JAK ODZYSKAĆ I ZABEZPIECZYĆ SWOJE KONTA

Komputer Świat

KONIEC PRZEMOCY W INTERNECIE

- Co zrobić, gdy nasze konto ktoś przejął
- Stalking a mobbing: czy to to samo
- Gotowe wnioski zgłoszeń na policję

WARTO WIEDZIEĆ:

RADZI KANCELARIA ANDERSEN TAX & LEGAL

▸ Najnowsze **przepisy prawa** w sprawach nękania

▸ **Kim** zazwyczaj **jest** nasz **prześladowca**

▸ Jak skutecznie zabezpieczyć **swoje konta w sieci**

▸ Jak zbierać dowody, **by uznał je sąd** i policja

NAJNOWSZE PRZEPISY W SPRAWACH

Przestępstwo nękania, zwane też stalkingiem, zostało wprowadzone do polskiego Kodeksu karnego w 2011 roku. Niedawno zaostrzono odpowiedzialność za jego popełnienie. Nowe przepisy obowiązują od 31 marca 2020 roku. ***Na czym polega stalking i co grozi sprawcy, który dopuścił się tego przestępstwa?***

Stalking oznacza działanie polegające na cyklicznym, złośliwym lub mającym na celu ośmieszenie prześladowaniu kogoś, wywołujące u niego poczucie zagrożenia. Zjawisko to znane jest od dawna. Niemniej w Polsce szczegółowe badania nad nim po raz pierwszy przeprowadzono dopiero w 2009 roku na polecenie Ministerstwa Sprawiedliwości. Badania wykazały, że skala zjawiska stalkingu w Polsce jest bardzo duża. Ofiarą uporczywego nękania padł bowiem co dziesiąty respondent. Uporczywe nękanie trwało przeciętnie rok (najczęściej od tygodnia do 3 miesięcy). Aż 15 procent ofiar było dręczonych przez co najmniej 3 lata, a co piąta oświadczyła, że trwa ono nadal (A. Siemaszko (red.), Stosowanie prawa. Księga jubileuszowa z okazji XX-lecia Instytutu Wymiaru Sprawiedliwości, Wolters Kluwer Polska).
Powyższe szokujące wyniki sprawiły, że ustawą z dnia 25 lutego 2011 roku wprowadzono do polskiego Kodeksu karnego nowy typ czynu zabronionego, jakim jest stalking.

Na czym polega stalking?

Stalking jest obecnie przestępstwem uregulowanym w art. 190a Kodeksu karego. Zgodnie z treścią tego przepisu:

§ 1. Kto przez uporczywe nękanie innej osoby lub osoby jej najbliższej wzbudza u niej uzasadnione okolicznościami poczucie zagrożenia, poniżenia lub udręczenia lub istotnie narusza jej prywatność, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§ 2. Tej samej karze podlega, kto, podszywając się pod inną osobę, wykorzystuje jej wizerunek, inne jej dane osobowe lub inne dane, za pomocą których jest ona publicznie identyfikowana, w celu wyrządzenia jej szkody majątkowej lub osobistej.

§ 3. Jeżeli następstwem czynu określonego w § 1 lub 2 jest targnięcie się pokrzywdzonego na własne życie, sprawca podlega karze pozbawienia wolności od lat 2 do 12.

§ 4. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.

Pamiętaj!
Nie uznaje się za uporczywe wysłanie kilku wiadomości tekstowych czy też kilku prób nawiązania połączenia telefonicznego. Przyjmuje się również, że dopiero w momencie, gdy ofiara żąda zaprzestania nękania, spełnione jest znamię uporczywości. Dlatego nie bój się powiedzieć stalkerowi STOP!

Przejawem stalkingu są między innymi natrętne próby komunikacji z ofiarą wbrew jej woli, niepożądane propozycje spotkań, udostępnianie na jej profilu wulgarnych lub obraźliwych treści aż po formułowanie gróźb. Za stalking uznaje się również natrętne wysyłanie esemesów czy maili, śledzenie, nawiązywanie połączeń głosowych, hałasowanie, zakłócanie spokoju, uniemożliwianie odpoczynku. Często adresatem wiadomości jest nie tylko osoba prześladowana, ale również jej bliscy.

Naruszenie prywatności

Przypisanie odpowiedzialności za stalking może mieć miejsce nie tylko w sytuacji, gdy zachowanie sprawcy uporczywego nękania wywołuje u ofiary poczucie zagrożenia, ale również, gdy prowadzi do istotnego naruszenia jej prywatności rozumianej jako wolność od ingerencji w życie prywatne, rodzinne i domowe, niezależnie do tego, czy dotyczy faktów obojętnych czy kłopotliwych. Naruszenie prywatności następuje z momentem określonego działania sprawcy, wkraczającego w sferę życia prywatnego pokrzywdzonego, na przykład poprzez nagrania lub fotografowanie. Jednak, aby zostało uznane za stalking, musi się powtarzać i wywoływać poczucie zagrożenia.

Podszywanie się pod inną osobę

Za formę stalkingu uznaje się również podszywanie się pod inną osobę lub wykorzystywanie jej wizerunku (art. 190a § 2 Kodeksu karnego). Zachowaniem takim jest między innymi zakładanie fałszywych kont na portalach społecznościowych, przedstawianie się nazwiskiem innej osoby w rozmowach telefonicznych czy publikowanie w sieci treści z podpisem innej osoby. Takie zachowanie musi być podjęte bez wiedzy i zgody osoby, której tożsamości się używa. Co więcej, wymaga się, by sprawca faktycznie dane lub wizerunek innej osoby wykorzystał poprzez wprowadzenie w błąd odbiorcy informacji. Należy pamiętać, że takie działanie musi być podejmowane w celu wyrządzenia szkody majątkowej lub osobistej. Szkoda taka finalnie nie musi jednak powstać.

Pamiętaj!
Żeby pociągnąć stalkera do odpowiedzialności za podszywanie się, wystarczy, by działanie takie podjął jednokrotnie.

Kodeks karny nie definiuje pojęcia nękania. Wskazuje natomiast na charakterystyczne cechy zachowania stalkera, które muszą zostać spełnione, by można było o nim mówić. Jak wynika z przytoczonego powyżej art. 190a, żeby zachowanie sprawcy zostało uznane za stalking:

- ***musi być uporczywe, co oznacza, że musi trwać przez określony czas, być intensywne, natarczywe i nachalne, a co najistotniejsze musi odbywać się wbrew woli ofiary;***
- ***musi wywoływać u ofiary poczucie zagrożenia, poniżenia, udręczenia lub naruszać jej prywatność.***

NĘKANIA

Fot. Simpson33/iStockphoto.com

Według Sądu Najwyższego, działania sprowadzające się do obserwacji, filmowania i fotografowania pokrzywdzonych spoza ich posesji, zamykające się tylko w sferze prywatnego dokumentowania, nieużywane do ściągnięcia na pokrzywdzonych jakiegokolwiek wymiernego zagrożenia, nie wypełniają znamienia poczucia zagrożenia z art. 190a § 1 k.k. Mogą jednak stanowić istotne naruszenie prywatności (wyrok z dnia 29.03.2017 r., wydany w sprawie prowadzonej pod sygnaturą V KK 413/16).

Kara więzienia dla stalkera

Za uporczywe nękanie oraz za kradzież tożsamości grozi kara pozbawienia wolności. Od 31 marca 2020 roku za popełnienie tych przestępstw stalker może pójść do więzienia na okres od 6 miesięcy aż do 8 lat. Jeśli wskutek jego działań pokrzywdzony targnął się na swoje życie, kara jest jeszcze surowsza – wynosi od 2 do 12 lat pozbawienia wolności. Ofiara może uzyskać również zakaz zbliżania się sprawcy.

Złóż wniosek o ściganie

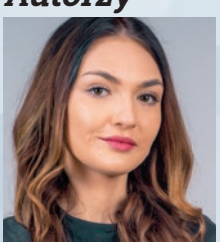
Co zrobić, żeby ukarać stalkera? Musisz w tym celu złożyć wniosek o jego ściganie. Możesz go złożyć na piśmie lub ustnie do protokołu. W piśmie należy wskazać:

- Dane organu, do którego składasz zawiadomienie (jednostka policji lub prokuratury właściwa według miejsca popełnienia przestępstwa);
- Swoje dane: imię, nazwisko, adres korespondencyjny, numer telefonu;
- Opis zdarzenia, o którym zawiadamiasz, w tym kiedy i gdzie miało ono miejsce;
- Dane sprawcy, jeżeli je posiadasz – w przypadku przestępstw popełnianych w sieci, sprawca pozostaje zwykle anonimowy, jednak organy ścigania podejmują próbę ustalenia jego tożsamości na podstawie numeru IP;
- Wysokość szkody, jeżeli wskutek opisanego w zawiadomieniu zdarzenia ją poniosłeś;
- Dane ewentualnych świadków;
- Dowody wskazujące na popełnienie przestępstwa (o tym, co może być dowodem popełnienia przestępstwa, przeczytaj w artykule pt. Jak zbierać dowody, by uznał je sąd i policja?" na stronie 10).

Pamiętaj! Z wniosku musi wynikać wola ścigania sprawcy, dlatego należy ją wyraźnie wyartykułować.

Jeśli chcesz złożyć zawiadomienie o przestępstwie w formie ustnej, musisz udać się do jednostki policji lub prokuratury. Zostaniesz wówczas poproszony o podanie informacji takich samych, jakie musiałbyś podać w zawiadomieniu pisemnym. Gdy zawiadomienie wysyłasz pocztą, wyślij je listem poleconym, najlepiej za potwierdzeniem odbioru.

Autorzy



KLAUDIA RACZEK
Prawnik w Kancelarii Andersen

NATALIA GAWEŁ
Adwokat w Kancelarii Andersen

KIM NAJCZĘŚCIEJ JEST TWÓJ PRZEŚLADOWCA?

Zjawisko stalkingu nieustannie przybiera na sile. Szacuje się, że ***od 12 do 16 procent kobiet i od 4 do 7 procent mężczyzn będzie prześladowanych przez stalkera w ciągu swojego życia****. Żeby uchronić się przed nim, warto wiedzieć, kto może nim być*

Stalking jako zjawisko społeczne występuje najprawdopodobniej od wieków. Słowo to pochodzi z języka angielskiego. Początkowo oznaczało wyłącznie podchody, skradanie się, tropienie i używane było głównie przez myśliwych zajmujących się polowaniem na dziką zwierzynę. Całkowicie nowego znaczenia nabrało w latach osiemdziesiątych XX wieku, kiedy to amerykańskie media zaczęły nagłaśniać przypadki obsesyjnego podążania przez fanów za hollywoodzkimi gwiazdami filmowymi, muzycznymi czy innymi osobami cieszącymi się popularnością wśród społeczeństwa (tzw. celebrity stalkers). Wówczas zaczęto go używać dla określenia formy nękania drugiego człowieka. Ofiarą stalkingu padł między innymi John Lennon, który w grudniu 1980 roku pod swoim domem na Manhattanie został zastrzelony przez uporczywie śledzącego go psychofana Marka Davida Chapmana. Stalkingu doświadczyła też Kasia Tusk czy Kuba Wojewódzki.

Kim jest stalker?

Złośliwa sąsiadka z piętra niżej waląca w rury, rozpowiadająca plotki na twój temat i ciągle wzywająca policję z powodu głośnych imprez, których nie urządzasz. Tajemniczy wielbiciel, który od miesięcy wysyła ci kwiaty do pracy i wiadomości z prośbą o kontakt na wszystkich możliwych portalach społecznościowych, a kiedy go zablokujesz, zakłada nowe konto. Koleżanka z klasy wyśmiewająca cię na każdym kroku. Były partner lub partnerka, który na zmianę wystaje pod twoim domem, błagając o powrót, a potem wyzywa od najgorszych. Każdy z nich może być twoim stalkerem.

Statystyki wskazują, że najczęściej prześladowca zna swoją ofiarę. Często jest to osoba nieszczęśliwie zakochana, której uczucia zostały odrzucone, lub były partner/partnerka. Może nim jednak być również ktoś, kogo znamy tylko z widzenia, ktoś zupełnie nieznajomy lub osoba, z którą mieliśmy zaledwie jednorazowy kontakt.

Statystyczny stalker to mężczyzna (około 80 procent) w wieku od 20 do 40 lat (D. Jędrek, Stalking w świetle badań empirycznych, [w:] Stalking). Większość sprawców wykazuje zaburzenia osobowości. Często są to osoby o skłonnościach narcystycznych, które łatwo się irytują i nie potrafią znieść odrzucenia.

Fot. Rafael Abdrakhmanov/iStockphoto.com

Typy prześladowców według Mullena

Przez lata specjaliści z dziedzin psychiatrii i psychologii dokonali podziału stalkerów ze względu na sposób ich zachowania i cechy osobowości. Najpopularniejsza jest typologia zaproponowana przez psychiatrów z Australii w zespole P.E. Mullena, M. Pathé i R. Purcell. Zaproponowali oni podział prześladowców na pięć grup: chcących nawiązać więź z ofiarą, odrzuconych, nieudolnych zalotników, rozgoryczonych i drapieżnych.

Uczuciowiec

Stalker uczuciowy (*intimacy seekers*) to prawdopodobnie najliczniejsza grupa sprawców uciążliwego nękania. Często są to osoby samotne, które poszukują relacji z ofiarą. Zwykle prześladują najdłużej – nękanie może trwać nawet kilka lat. Ich celem jest nawiązanie więzi, rozwinięcie jej, a następnie przejście na „nowy poziom" znajomości. Stalker jest zwykle znajomym ofiary (choć nie zawsze) i swoimi działaniami próbuje pogłębić łączącą go z nią więź wbrew jej woli. Prześladowcy tego typu uważają, że dzięki swoim natarczywym działaniom zdobędą przychylność drugiej osoby. Bronią się przed uczuciami upokorzenia, wstydu i smutku narcystyczną wściekłością.

Odrzucony

Liczną grupę stalkerów stanowią też odrzuceni (*rejected stalkers*). Najczęściej są to osoby, które przeżyły zawód miłosny (zakończenie związku, odrzucenie przez partnera, zazdrość o nowego partnera) lub które zakończyły inną bliską relację. Ofiarą odrzuconego stalkera może być przykładowo były przyjaciel, kole-

Fot. Sam Thomas/iStockphoto.com

żanka z pracy przeniesiona do innego działu czy nawet terapeuta, który odmówił prowadzenia dalszej terapii. Odrzucony prześladowca nie może się pogodzić z rozpadem relacji, jest zaborczy, często śledzi swoją ofiarę. Z jednej strony błaga o przebaczenie i powrót, obdarowując prezentami. Z drugiej strony jest agresywny i wulgarny – wyzywa, a nawet posuwa się do rękoczynów. Innym razem przejawia zachowania depresyjne i smutek. Odrzuceni sprawcy są wytrwali i intensywni w prześladowaniach.

Nieudolny zalotnik

Są jeszcze nieudolni zalotnicy (*incompetent suitors*). To osoby, których problemy wynikają przede wszystkim ze słabych umiejętności społecznych i potrzebą zwrócenia na siebie uwagi. Dążą do nawiązania relacji z inną osobą – zwykle na początku chodzi im jedynie o randkę. Uważają, że „nie" znaczy „tak", a odmowę ofiary uznają za flirt. Odrzucony zalotnik nęka ofiarę, mając nadzieję, że w końcu zgodzi się na spotkanie. Wśród nieudolnych zalotników wielu sprawców to „recydywiści", mający często wiele ofiar na koncie. Okres nękania jest jednak stosunkowo krótki – zniechęceni poszukują nowych obiektów, z którymi chcą wejść w związek.

Urażony

Urażeni prześladowcy (*resentful stalkers*) to grupa sprawców, którzy czują się skrzywdzeni przez życie. Nieustannie mszczą się za doznane krzywdy, dążąc do tego, by ofiara cierpiała tak jak oni. Często działają przypadkowo, wybierają ją losowo (na przykład przypadkowo spotkana na ulicy atrakcyjna kobieta, którą prześladowca zaczyna nękać, ponieważ inna kobieta go odrzuciła). Nierzadko jednak ich ofiarami są osoby, które upokorzyły ich w przeszłości lub same znęcały się nad stalkerem (na przykład szkolni prześladowcy). Wszelkie kary nakładane za ich działania sprawiają, że czują się jeszcze bardziej pokrzywdzeni, co podsyca ich zapał do dalszych działań prześladowczych.

Drapieżca

Drapieżcy (*predatory stalkers*) stanowią najmniej liczną i jednocześnie najgroźniejszą grupę stalkerów. Ze względu na wyrafinowany sposób działania, to właśnie oni zdobywają rozgłos. Metodycznie dążą do osiągnięcia każdego celu. Osoba będąca celem często nawet nie zdaje sobie sprawy z faktu, że jest obserwowana. Jest to bowiem typ prześladowcy, który nie ujawnia się, dopóki nie nadejdzie „odpowiednia chwila". Wielu drapieżców było już wcześniej karanych, a połowa z nich dokonała już napaści na ofiarę.

Ignoruj zachowanie stalkera

Zdaniem psychologów motywacją stalkerów, która napędza ich do dalszego działania, jest reakcja na ich zachowanie. Kluczową kwestią jest więc ich ignorowanie, nieprzyjmowanie prezentów i nieodpisywanie na wiadomości. Jeżeli podejrzewasz, że masz do czynienia z prześladowcą, koniecznie poinformuj o tym policję.

Autorka

KINGA RABĘDA
Aplikant radcowski
w Kancelarii Andersen

MOBBING A STALKING – CZY TO TO

Zarówno stalking, jak mobbing są niepożądanymi zjawiskami społecznymi, mogącymi doprowadzić do uszczerbku na zdrowiu psychicznym i fizycznym. *Sytuacji noszących znamiona tych zjawisk nie należy bagatelizować. Z racji tego, że nie są to pojęcia tożsame, należy każdorazowo ocenić, z którym z nich mamy do czynienia, by wybrać właściwą drogę dochodzenia swoich praw*

Nie od dziś wiadomo, że ludzie potrafią być względem siebie nawzajem złośliwi. Czasem mają do tego powody – mniej lub bardziej uzasadnione, a czasem bywają niemili jedynie dla zasady. Takie zachowania – bez względu na ich przyczynę – zwykle odciskają piętno na osobie, względem której są kierowane. Jest tak zwłaszcza wtedy, gdy dane zachowanie nie jest jednorazowym incydentem, lecz powtarza się na tyle często, że staje się uciążliwe. Może zostać wówczas zakwalifikowane jako stalking lub mobbing.

Analiza sprawców pozwoliła na wyróżnienie schematów ich zachowań, które, podejmowane długotrwale i łącznie, mogą być zakwalifikowane jako przestępstwo stalkingu. Są to między innymi: wysyłanie uporczywych listów (zarówno w formie tradycyjnej, jak i e-mail), esemesów, uporczywe dzwonienie, głuche telefony, śledzenie, nachodzenie w miejscu pracy lub w miejscu, w którym ofiara regularnie przebywa, wypytywanie o ofiarę w otoczeniu czy rozpowszechnianie o niej nieprawdziwych informacji.

Stalking

Stalking jest przestępstwem uregulowanym w art. 190a Kodeksu karnego. Polega na upor czywym nękaniu innej osoby lub osoby jej najbliższej, prowadzącym do wywołania u niej uzasadnionego okolicznościami poczucia zagrożenia, poniżenia, udręczenia lub istotnego naruszenia jej prywatności. Stalking to również podszywanie się pod inną osobę, wykorzystywanie jej wizerunku lub danych, za pomocą których jest ona publicznie identyfikowana, w celu wyrządzenia jej szkody majątkowej lub osobistej. W świadomości społeczeństwa jest utożsamiany z formą przemocy emocjonalnej. Za jego popełnienie grozi kara pozbawienia wolności od 6 miesięcy do 8 lat. W przypadku gdy ofiara targnie się na swoje życie, odpowiedzialność karna jest zaostrzona i kara pozbawienia wolności wynosi od 2 do 12 lat.

W ostatnich latach skala zjawiska stalkingu istotnie wzrosła. Głównie poprzez upowszechnienie się dostępu do internetu, który zapewnia pozorną anonimowość i daje prześladowcom złudne poczucie bezkarności. Nękanie w sieci to tak zwany cyberstalking. Polegać może na zamieszczaniu kompromitujących ofiarę zdjęć lub komentarzy na portalach społecznościowych. Jako stalking kwalifikowana jest również kradzież tożsamości, która najczęściej przejawia się w przejęciu lub założeniu fałszywego konta na Facebooku, Instagramie czy innym portalu. Stalker często śledzi swoją ofiarę, wykorzystując informacje zebrane na jej temat w sieci, na przykład dzięki aplikacjom pokazującym, jakie trasy pokonuje ona podczas treningów, czy funkcjom portali społecznościowych, których ofiara używa do oznaczania swojej aktualnej lokalizacji.

Ściganie stalkingu następuje na wniosek pokrzywdzonego (z urzędu, gdy ofiara targnęła się na swoje życie). Oprócz podjęcia działań w celu ukarania stalkera możesz również wystąpić z pozwem do sądu cywilnego o naruszanie dóbr osobistych, żądając zakazania mu dalszych podobnych działań, a także zasądzenia od niego na twoją rzecz zadośćuczynienia lub odszkodowania.

Więcej szczegółów na temat przestępstwa stalking znajdziesz w artykule Najnowsze przepisy w sprawach nękania na stronach 2–3.

Fot. Manuel-F.-O./iStockphoto.com

Mobbing

W odróżnieniu od stalkingu, mobbing jest pojęciem wywodzącym się z prawa pracy. Został zdefiniowany w art. 94[3] § 2 Kodeksu pracy. Zgodnie z treścią wskazanego przepisu, mobbing oznacza działania lub zachowania dotyczące pracownika lub skierowane przeciwko pracownikowi, które łącznie:

- polegają na jego uporczywym i długotrwałym nękaniu lub zastraszaniu,
- wywołują u niego zaniżoną ocenę przydatności zawodowej,
- powodują lub mają na celu jego poniżenie lub ośmieszenie, izolowanie go lub wyeliminowanie z zespołu współpracowników.

Cechą charakterystyczną dla mobbingu jest bezpośrednie powiązanie zachowania sprawcy z miejscem pracy – jego sprawcą może być pracodawca, twój przełożony lub współpracownik, a ty musisz posiadać status pracownika.

SAMO?

Fot. Grinvalds/iStockphoto.com

Mobbing może polegać na ośmieszaniu lub poniżaniu pracownika, izolowaniu go, eliminowaniu z zespołu (na przykład poprzez odsunięcie go od ciekawych i pożądanych przez pracownika projektów) lub też zarzucaniu pracownika nadmierną ilością zadań. Pamiętaj! Pojęcie mobbingu nie obejmuje działań pracodawcy, które są dozwolone prawem. Mobbingu nie stanowi zatem poddanie pracownika przez pracodawcę krytycznej, ale konstruktywnej ocenie, którego celem nie jest poniżenie pracownika, ale zwrócenie mu uwagi na popełniane błędy.

Co bardzo istotne, obowiązek udowodnienia, że w danej sytuacji doszło do mobbingu, spoczywa na pracowniku. Dlatego, jeśli jesteś jego ofiarą, musisz zbierać dowody potwierdzające, że jesteś nękany lub zastraszany.

Pracownik, u którego mobbing wywołał rozstrój zdrowia, może dochodzić od pracodawcy odpowiedniej sumy tytułem zadośćuczynienia pieniężnego za doznaną krzywdę lub odszkodowania.

STALKING A MOBBING – RÓŻNICE I PODOBIEŃSTWA

	Stalking	Mobbing
Reżim odpowiedzialności	Kodeks karny	Kodeks pracy
Forma czynu	Przemoc emocjonalna	Przemoc emocjonalna
Sprawca	Każdy	Pracodawca lub współpracownik
Ofiara	Każdy	Pracownik
Cechy czynu	Uporczywość	Długotrwałość, uporczywość
Skutki czynu	Wywołanie poczucia zagrożenia, poniżenia, udręczenia lub istotnego naruszenia prywatności	Wywołanie zaniżonej oceny przydatności zawodowej, poniżenia lub ośmieszenia, izolowania lub wyeliminowanie z zespołu współpracowników
Możliwe działania	■ Złożenie wniosku o ściganie stalkera ■ Wystąpienie z pozwem cywilnym o naruszenie dóbr osobistych. Jeżeli działanie stalkera wyrządziło szkodę, w pozwie można dochodzić odszkodowania	■ Wystąpienie z pozwem do sądu pracy o zadośćuczynienie, gdy mobbing wywołał rozstrój zdrowia, lub o odszkodowanie

Autorzy

NATALIA GAWEŁ
Adwokat w Kancelarii Andersen

MAGDALENA KĘSKA
Aplikant radcowski w Kancelarii Andersen

Stalking w pracy – czy jest możliwy?

Wspólną cechą stalkingu i mobbingu jest uporczywe nękanie, które zarówno w pierwszym, jak i drugim przypadku negatywnie wpływa na osobę, do której zachowanie takie jest kierowane. Dlatego nie można wykluczyć, że dane zachowanie pracodawcy czy współpracownika jednocześnie nie zostanie zakwalifikowane jako każdy z tych czynów.

Przykładem zachowania spełniającego cechy mobbingu i stalkingu może być permanentne obciążanie pracownika (częściej niż innych pracowników) nadmierną ilością zadań, które – żeby im sprostać – musi wykonywać po godzinach, przy jednoczesnym:

- ponaglaniu go w ich realizacji poprzez dzwonienie i wysyłanie do niego maili czy esemesów w środku nocy,
- nachodzeniu go po godzinach pracy, żeby przypomnieć mu, że powinien pracować zamiast odpoczywać,
- przypominaniu mu na każdym kroku, że nie nadaje się do wykonywanej pracy i że powinien zostać zwolniony.

To dosyć skrajny przypadek, ale i takie się zdarzają. Pracownik, który doświadczył takich zachowań, może dochodzić zarówno pociągnięcia sprawcy do odpowiedzialności karnej za stalking, jak i żądać od pracodawcy odszkodowania i zadośćuczynienia z tytułu mobbingu.

CO ZROBIĆ, GDY KTOŚ PRZEJĄŁ TW

Gdy zauważysz, że ktoś korzysta z twojego konta na portalu społecznościowym albo że w twojej skrzynce mailowej znajdują się wiadomości uznane za odczytane, pomimo że jeszcze ich nie czytałeś, ***najprawdopodobniej ktoś włamał się na twoje konto***

Internet jest obecnie podstawowym narzędziem komunikacji. Do porozumienia się wykorzystujemy pocztę elektroniczną, komunikatory, konta na rozmaitych portalach społecznościowych i czatach. Używamy ich nie tylko w relacjach prywatnych, ale także w kontaktach biznesowych. Jakie działania należy podjąć, gdy ktoś nielegalnie uzyska do nich dostęp?

Jak działa przestępca?

Do włamań na cudze konta internetowe dochodzi głównie wskutek wyłudzenia danych logowania. Następuje to zwykle poprzez wysłanie do potencjalnej ofiary wiadomości zawierającej link nakłaniający do podjęcia określonych działań lub mający na celu zainfekowanie jej komputera złośliwym oprogramowaniem (tak zwany phishing). Równie częste są przypadki crackingu (nie mylić z hakingiem!), polegające na łamaniu zabezpieczeń do systemów komputerowych (haseł, kodów, pinów etc.). Nierzadko dochodzi również po prostu do odgadnięcia hasła dostępowego (na przykład do profilu na portalu społecznościowym), co ma miejsce, zwłaszcza gdy sprawca zna swoją ofiarę, a co za tym idzie – zna jej preferencje, wybory czy poprzednie hasła.

Po co mu dostęp do twojego konta?

Kolega włamuje się na profil koleżanki, żeby opublikować na nim zabawny post na jej temat. Siostra czyta maile starszego brata, żeby dowiedzieć się, kim jest jego nowa dziewczyna. Do włamań na konta na portalach społecznościowych czy na skrzynki e-mail niejednokrotnie dochodzi z ciekawości czy dla zabawy. Zwykle działania takie są jednorazowe, nie są szkodliwe społecznie, choć **zawsze stanowią naruszenie prywatności, w tym objętej nią tajemnicy korespondencji**.

W ostatnim czasie do przejęcia kont internetowych coraz częściej dochodzi jednak w celach przestępczych. Stalkerzy wykorzystują je jako narzędzie służące do nękania ofiary. Za pośrednictwem skradzionego konta wysyłają do jej znajomych zawierające nieprawdziwe informacje wiadomości, publikują ośmieszające ją posty lub po prostu uniemożliwiają jej dostęp do niego. Więcej na temat stalkingu przeczytasz w artykule Najnowsze przepisy w sprawach nękania na stronie 2.

Konta na portalach społecznościowych nieraz służą też wyłudzaniu pieniędzy. Znane są sytuacje, w których przestępca przejmował konto, zmieniał jego ustawienia i żądał pieniędzy za jego oddanie właścicielowi z powrotem do używania. Co więcej, co najmniej kilku moich znajomych w ostatnim czasie padło również ofiarą tak zwanego oszustwa na BLIKA. Oszust włamywał się na ich konto na Facebooku i podając się za nich, wysyłał do ich znajomych prośby o przekazanie pieniędzy poprzez podanie kodu BLIK. Ofiara podaje kod, akceptuje płatność w aplikacji bankowej, a oszust dostaje pieniądze. Na szczęście nikt spośród nich nie nabrał się na ten numer, choć oszuści potrafią być przekonujący.

Art. 268a Kodeksu karnego

§ 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3.

§ 2. Kto, dopuszczając się czynu określonego w § 1, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 3. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.

Jak się chronić?

Zgodnie z zasadą lepiej zapobiegać niż leczyć, warto już dzisiaj zabezpieczyć swoje konto internetowe przed niepożądanym dostępem ze strony osób trzecich. Z pewnością dzięki temu unikniesz stresu związanego z jego odzyskiwaniem, tłumaczeniem innym, co się na nim dzieje, i co najważniejsze – uchronisz znajdujące się na nim dane. Nie od dziś przecież wiadomo, że konta internetowe są kopalnią wiedzy na nasz temat – to kolejny powód, dla którego cyberprzestępcy pożądają dostępu do nich.

Złóż zawiadomienie o przestępstwie

Gdy okaże się, że ktoś uzyskał nielegalnie dostęp do twojego profilu na portalu społecznościowym, poczty elektronicznej, konta na czacie lub komunikatora, złóż zawiadomienie o popełnieniu przestępstwa. Możesz, a nawet powinieneś to zrobić, zarówno gdy do włamania doszło, bo twoje konto internetowe było niewystarczająco zabezpieczone, jak i wtedy, gdy je zabezpieczyłeś, ale okazało się, że masz do czynienia z wytrawnym przestępcą, który jest w stanie uzyskać dostęp nawet do kont NASA.

Zawiadomienie możesz złożyć na piśmie lub ustnie do protokołu w najbliższej jednostce policji lub prokuratury. Należy w nim wskazać:

- Dane organu, do którego składasz zawiadomienie (jednostka policji lub prokuratury właściwa według miejsca popełnienia przestępstwa);
- Swoje dane: imię, nazwisko, adres korespondencyjny, numer telefonu;
- Opis zdarzenia, o którym zawiadamiasz, w tym kiedy i gdzie miało ono miejsce;

NIE DAJ SIĘ OSZUSTOWI!

- Zainstaluj na swoim komputerze oprogramowanie antywirusowe i antyspamowe. Pamiętaj o jego aktualizowaniu!
- Zabezpiecz konto hasłem. Unikaj haseł prostych, które łatwo można złamać, i cyklicznie je zmieniaj. Nikomu ich nie podawaj!
- Nigdy nie klikaj na podejrzane linki. Zamiast tego wpisz adres WWW ręcznie do wyszukiwarki.
- Sprawdź, czy adres strony internetowej, na którą przekierował cię link, zawiera w pasku adresowym protokół https, oznaczający połączenia szyfrowane, zamiast protokołu http. Jedynie protokół https pozwala na bezpieczne przesyłanie danych.
- Jeśli otrzymałeś podejrzaną wiadomość, sprawdź jej nadawcę – skontaktuj się z podmiotem, od którego ma pochodzić wiadomość, i ustal, czy rzeczywiście ją do ciebie wysłał.
- Nie dodawaj do listy kontaktów przypadkowych, nieznanych ci osób.

OJE KONTO W SERWISIE ONLINE?

- Wysokość szkody, jeżeli wskutek opisanego w zawiadomieniu zdarzenia ją poniosłeś;
- Dane ewentualnych świadków;
- Dowody wskazujące na popełnienie przestępstwa, na przykład wydrukowane wiadomości, które oszust wysłał do twoich znajomych, próbujący wyłudzić od nich pieniądze, czy wiadomość, w której żąda pieniędzy za przywrócenie dostępu do twojego konta. Więcej na temat dowodów przeczytasz w artykule Jak zbierać dowody, by uznał je sąd i policja? na stronie 10.

Pamiętaj! Z racji tego, że omawiane przestępstwa są ścigane na wniosek, w zawiadomieniu musisz wyraźnie wyartykułować wolę ścigania sprawcy.

Kodeks postępowania karnego nie określa formy, w jakiej pokrzywdzony powinien wyrazić wolę ścigania (to jest złożyć wniosek); wola ta może być wyrażona ustnie do protokołu zawiadomienia o przestępstwie czy do protokołu przesłuchania w charakterze świadka albo przez własnoręcznie sporządzone pismo lub przez podpisanie odpowiednio przygotowanego formularza (druku); istotne bowiem jest to, by z dokumentu procesowego w sposób wyraźny wynikało żądanie pokrzywdzonego ścigania sprawców (wyrok Sądu Najwyższego z dnia 12 grudnia 1985 r. II KR 372/85).

Co dalej?

Wskutek zawiadomienia o popełnieniu przestępstwa organy ścigania będą prowadziły postępowanie przygotowawcze między innymi w celu wykrycia i w razie potrzeby ujęcia sprawcy. Jeżeli sprawca nie zostanie ustalony, postępowanie zostanie umorzone – taką decyzję możesz zaskarżyć! Jeśli natomiast uda się ustalić jego tożsamość, sprawa trafi do sądu. Pamiętaj, że w postępowaniu sądowym, aż do zamknięcia przewodu sądowego, możesz zgłosić wniosek o naprawie szkody, jaka została ci wyrządzona wskutek przestępstwa. W takim przypadku sąd ukarze sprawcę, zobowiązując go jednocześnie do pokrycia szkody. Jeżeli nie zgłosisz takiego wniosku w postępowaniu karnym albo sąd karny nie orzeknie co do całości żądanej przez ciebie kwoty, nic straconego. Możesz jeszcze raz wnieść pozew do sądu cywilnego.

A może pozew o naruszenie dóbr osobistych?

Wskutek włamania na twoje konto dochodzi do naruszenia twojej prywatności, w tym tajemnicy korespondencji. Stanowią one dobra osobiste i podlegają ochronie. Dlatego, jeśli znasz tożsamość sprawcy, możesz wytoczyć przeciwko niemu pozew o naruszenie dóbr osobistych.

W pozwie możesz żądać zaniechania dalszych działań polegających na naruszaniu twoich dóbr, a także wykonania czynności potrzebnych do usunięcia jego skutków. W szczególności możesz żądać, żeby sprawca złożył oświadczenie odpowiedniej treści i w odpowiedniej formie (na przykład przeprosiny w Komputer Świecie lub innym czasopiśmie). Możesz też żądać zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy pieniężnej na wskazany przez ciebie cel społeczny. O ile wcześniej nie zobowiązano już sprawcy do naprawienia wyrządzonej ci szkody, możesz też żądać odszkodowania.

Gdy sąd – karny lub cywilny – zasądzi na twoją rzecz żądaną kwotę odszkodowania, sprawca przestępstwa powinien ją niezwłocznie uregulować. Jeżeli nie zrobi tego dobrowolnie, w celu jej wyegzekwowania możesz skorzystać z pomocy komornika.

Fot. Tero Vesalainen/iStockphoto.com

Autorka

NATALIA GAWEŁ
Adwokat w Kancelarii Andersen

JAK ZBIERAĆ DOWODY, BY UZNAŁ JE

Coraz częściej padamy ofiarą cyberprzestępców. Rzadko jednak decydujemy się na dochodzenie sprawiedliwości i zgłaszanie popełnianych przez nich przestępstw, z góry zakładając brak szans na wygraną w sądzie. Jednak ***gdy masz twarde dowody potwierdzające popełnienie przestępstwa, szanse na wykrycie i ukaranie sprawcy są całkiem realne****. Jak je zebrać, by zostały uznane za wiarygodne?*

Życie w sieci. . .

Obecnie nasze życie – zarówno towarzyskie, jak i zawodowe – w znacznej mierze toczy się w sieci (w dobie COVID-19 częściej niż zwykle). Dla większości ludzi rytuałem stało się umieszczanie dziesiątek zdjęć na portalach społecznościowych, na których dzielimy się ze znajomymi swoimi przeżyciami. Pokazujemy, co jemy, gdzie byliśmy i jak spędzamy czas wolny. Telefony, tablety i smartwatche stały się naszymi „centrami dowodzenia", bez których nie potrafimy się obyć i czujemy się jak „bez ręki". Dlatego można śmiało zaryzykować stwierdzenie, że życie dzieli się dzisiaj na dwa wymiary: realny – fizyczny, oraz wirtualny – w sieci, którego nie da się zmaterializować, a który istotnie wpływa na ten pierwszy.

. . .przestępstwa w sieci

Niestety, wraz z przeniesieniem się wielu aspektów naszego życia do sieci, w ślad za nimi do internetu podążyły też przestępstwa i nadużycia. Poza hakingiem, który prowadzi do utraty przez użytkowników danych umieszczanych w sieci, spotykamy się z coraz to nowymi nieuczciwymi praktykami. Przykładowo, otrzymujemy wiadomości mające na celu wyłudzenie pieniędzy czy też posłużenie się naszymi danymi osobowymi. Przychodzące na nasze skrzynki e-mailowe setki wiadomości próbują nakłonić nas do zainwestowania środków finansowych w inwestycję z 300-procentowym zwrotem czy też do zakupienia cudownego remedium na odchudzanie. Coraz częściej spotykamy się też z trollingiem internetowym czy stalkingiem. Kolejnym i wydaje się głównym powodem, który sprawia, że odwieczna walka dobra ze złem w przypadku przestępstw popełnianych w sieci jest tak trudna, jest konieczność ich udowodnienia. Jak zatem bronić się przed takimi przestępstwami i jak można je udowodnić przed organami ścigania?

Walka z przestępczością internetową nie jest łatwa. Wynika to z kilku niewiadomych, które prawie zawsze trzeba zidentyfikować. Są to:

- ***Miejsce popełnienia przestępstwa – z uwagi na fakt, że czyn popełniono w sieci, jego wskazanie jest często trudne;***
- ***Sprawca – ze względu na anonimowość, jaką zapewnia mu sieć, trzeba się nieraz mocno nagimnastykować, żeby ustalić jego tożsamość.***

Co może być dowodem?

Gdy padniemy ofiarą przestępstwa i zdecydujemy się na zawiadomienie o nim organów ścigania, musimy przedstawić dowody potwierdzające jego popełnienie. Jako dowód mogą posłużyć wszelkie środki, które pozwolą na dokonanie ustaleń mających znaczenie dla rozstrzygnięcia sprawy, a w rezultacie doprowadzą do zrealizowania zasady prawdy materialnej, zgodnie z którą orzeczenie ma być oparte na rzeczywistych ustaleniach faktycznych.

Brak jest wymogu, by wskazane powyżej nośniki informacji miały postać oryginału. Mogą one stanowić kopie. Dzięki temu, zamiast załączać do zawiadomienia o popełnieniu przestępstwa dysk twardy, na którym zapisano szkalujący twoje dobre imię e-mail, wystarczające będzie jego wydrukowanie. Nie można jednak wykluczyć, że w toku postępowania karnego organy ścigania zajmą komputer lub

Fot. Digicomphoto/iStockphoto.com

CO MOŻE BY BYĆ DOWODEM

W zależności od typu przestępstwa dowód mogą stanowić przede wszystkim:

- wiadomości e-mail,
- wiadomości otrzymane na Messengerze lub innym komunikatorze,
- komentarze pod zdjęciami czy postami publikowanymi na portalach społecznościowych,
- zdjęcia prezentujące ekran komputera, na którym widoczne są przestępcze treści,
- wydruki stron WWW, print screeny,
- wydruk prośby do administratora strony o zabezpieczenie danej wiadomości czy potwierdzenie komunikatu (szczególnie przydatne w przypadku przestępstw związanych z wyłudzeniem, gdy nadawcy wiadomości podszywają się na przykład pod instytucje finansowe),
- pliki komputerowe wpostaci zdjęć czy nagrań,
- nośniki elektroniczne, takie jak dyski twarde, pamięci USB, karty SD.

SĄD I POLICJA?

Fot. Maksym Panchuk/iStockphoto.com

inny nośnik informacji, na których zapisano oznaczone dane na czas jego trwania.

Czy każdy dowód jest dopuszczalny?

Granice zbierania dowodów, które mają służyć dochodzeniu sprawiedliwości, wyznaczają przepisy kodeksu postępowania karnego. Wynika z nich przede wszystkim, że dowody powinny być gromadzone w sposób niebudzący wątpliwości, muszą być wiarygodne i prawidłowo zabezpieczone. Oznacza to, że dowód elektroniczny dokumentujący popełnienie przestępstwa w sieci:

- **musi być autentyczny** – co oznacza, że źródło jego pochodzenia nie powinno budzić wątpliwości,
- **musi być wiarygodnie zabezpieczony** – co oznacza konieczność jego zabezpieczenia w sposób wykluczający możliwość ingerencji w jego treść,
- **musi zawierać treść potwierdzającą dokonanie czynu zabronionego**.

Pamiętaj! Wszelkie niedające się usunąć wątpliwości sąd rozstrzyga na korzyść oskarżonego. Dlatego dowód niespełniający powyższych wymogów najprawdopodobniej nie zostanie uwzględniony przez sąd. Sąd oddali również wniosek dowodowy, gdy:

- przeprowadzenie dowodu jest niedopuszczalne;
- okoliczność, która ma być udowodniona, nie ma znaczenia dla rozstrzygnięcia sprawy albo jest już udowodniona;
- dowód jest nieprzydatny do stwierdzenia danej okoliczności;
- dowodu nie da się przeprowadzić;
- wniosek dowodowy w sposób oczywisty zmierza do przedłużenia postępowania;
- wniosek dowodowy został złożony po za kreślonym przez organ procesowy terminie.

Gdy nie masz możliwości zabezpieczenia dowodu w oryginalnej wersji lub nie wiesz, jak to zrobić, zwróć się do wyspecjalizowanych podmiotów lub od razu do organów ścigania. Nie działaj na własną rękę, bo możesz zmodyfikować plik, co podważy jego wiarygodność.

Jak zabezpieczyć dowód?

Najważniejszą zasadą dotyczącą dowodów „elektronicznych" wykorzystywanych przed sądem jest wykluczenie jakichkolwiek możliwości ich modyfikacji. Dlatego przede wszystkim należy je zabezpieczyć. W przypadku wiadomości e-mail, powiadomień na Messengerze lub innych komunikatorach zabezpieczeniem będzie ich wydruk. **Pamiętaj, żeby oryginalną wiadomość pozostawić na serwerze lub programie pocztowym.** W żadnym wypadku ich nie kasuj! Tak samo należy postąpić, gdy ktoś publikuje złośliwe komentarze pod zdjęciami lub postami umieszczonymi na portalu społecznościowym czy na stronie WWW. Jeśli dowód znajduje się na nośniku elektronicznym (dysk twardy, pamięć USB, karta SD), wykonaj jego kopię binarną (tak zwany backup). Pojedyncze pliki komputerowe (na przykład zdjęcia, nagrania wideo) zabezpiecz, wykonując kopię całego nośnika, na którym zapisano plik.

Oprócz zabezpieczenia dowodów wskazujących na popełnianie przestępstwa należy również ustalić:

- kiedy wysłano wiadomość, post czy komentarz, stanowiący przestępstwo,
- kiedy zapoznaliśmy się z ich treścią,
- kto je wysłał lub opublikował – nie zawsze możliwe jest zidentyfikowanie sprawcy z imienia i nazwiska, ale często posługuje się on pseudonimem (nick),
- z jakiego adresu e-mail wysłano wiadomość,
- jeśli dowodem jest plik, kto i kiedy go stworzył oraz kto i kiedy wprowadzał jego modyfikacje.

Innymi słowy, powinniśmy ustalić i dołączyć do każdego z dowodów dotyczące go metadane.

Im więcej szczegółów dotyczących przestępstwa zdobędziesz i przedstawisz organom ścigania i sądowi, tym większe są szanse na ustalenie, a następnie ukaranie sprawcy. Dlatego gdy padniesz ofiarą cyberprzestępcy, nie daj się ponieść emocjom i działaj rozsądnie. Zabezpiecz dowody i idź na policję.

Autor

ADAM KSIĄŻEK
Aplikant radcowski
w Kancelarii Andersen

KTO MA DOSTĘP DO MOICH KONT?

Podejrzewacie, że ktoś ma dostęp do waszego konta na portalu społecznościowym lub poczcie? Być może zalogowaliście się gdzieś i zapomnieliście wylogować? Na szczęście ***wiele usług i serwisów pozwala monitorować logowania i wylogowywać się zdalnie***

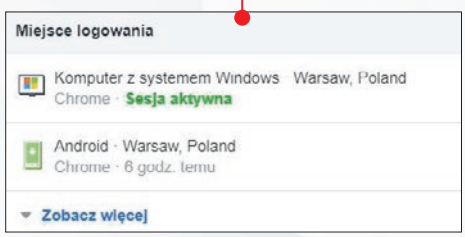
Dziś do serwisów społecznościowych czy skrzynek poczty elektronicznej logujemy się na przeróżnych urządzeniach w różnych miejscach. Od naszych smartfonów, przez służbowe laptopy aż po komputery naszych znajomych. Warto wiedzieć, czy gdzieś nie zostaliśmy zalogowani albo czy ktoś trzeci nie uzyskał dostępu do naszych kont. Na szczęście w większości przypadków łatwo to sprawdzić. Niestety, w większości serwisów funkcje te znajdują się w innych miejscach.

Facebook

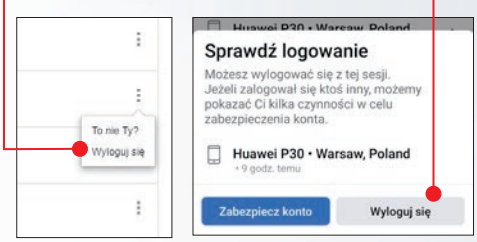
Największy serwis społecznościowy świata pozwala nie tylko sprawdzić, gdzie jesteśmy zalogowani, ale także wylogować się ze wszystkich urządzeń kilkoma kliknięciami. Opcje zarządzania w tym aspekcie odnajdziemy, rozwijając menu w prawym górnym rogu i wybierając opcję **Ustawienia i prywatność**, a następnie **Ustawienia**.

W przypadku wersji smartfonowej konieczne będzie naciśnięcie przycisku menu (trzy kreski w prawym górnym rogu), a następnie przewinięcie okna w dół, do pokazania się funkcji **Ustawienia i prywatność**. Po tym również wybieramy **Ustawienia**.

Teraz, niezależnie od platformy, wyszukujemy funkcję **Bezpieczeństwo i logowanie**. Możemy tam podejrzeć, na jakich urządzeniach jesteśmy lub byliśmy zalogowani. W celu wylogowania



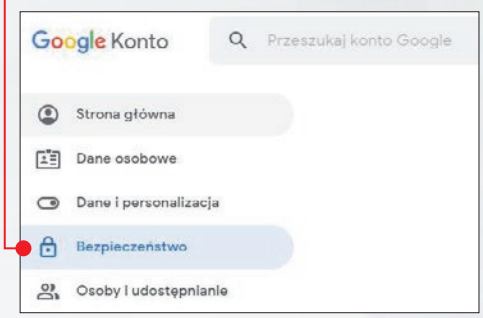
się z konkretnego urządzenia, klikamy na trzy kropki przy jego nazwie i wybieramy **Wyloguj się**. Działa to zarówno na komputerze, jak i smartfonie.



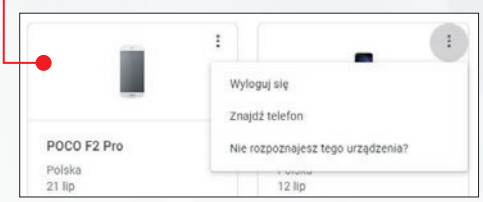
Gmail (Google)

W przypadku naszego konta Google, za pośrednictwem którego możemy korzystać między innymi z poczty Gmail czy mieć dostęp do kanału YouTube, także mamy możliwość szybkiego sprawdzenia, gdzie jesteśmy zalogowani. W tym celu klikamy na ikonę naszego profilu i wybieramy **Zarządzaj kontem Google**.

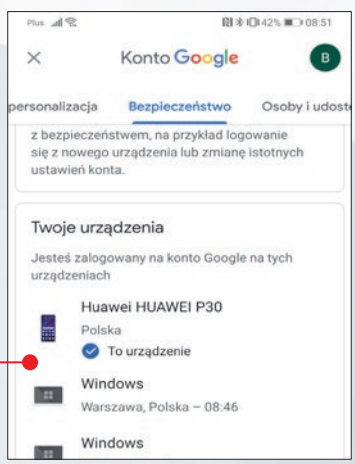
W nowo otwartym oknie znajdujemy zakładkę **Bezpieczeństwo** i w głównym oknie w polu



Twoje urządzenia wyświetlone będą miejsca, na których jesteśmy lub niedawno byliśmy zalogowani do naszego konta Google. Klikając na przycisk **Zarządzaj urządzeniami**, włączymy bardziej szczegółowy widok i będziemy w stanie wylogować się z konkretnych urządzeń. W tym celu konieczne jest kliknięcie na ikonę menu w postaci trzech kropek i wybranie opcji **Wyloguj się**.

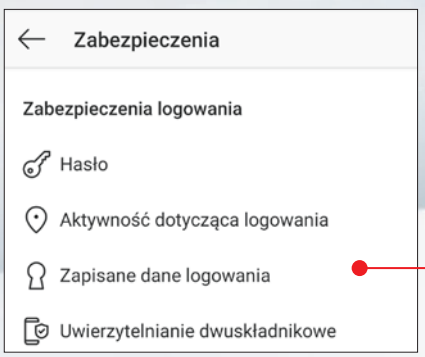


Analogicznie działa to na smartfonie. W aplikacji Google klikamy na naszą ikonę i wybieramy **Zarządzaj kontem Google**, następnie wśród zakładek znajdujemy **Bezpieczeństwo** i przesuwamy ekran, aż naszym oczom ukaże się widok urządzeń, na których możliwy był dostęp do naszego konta.

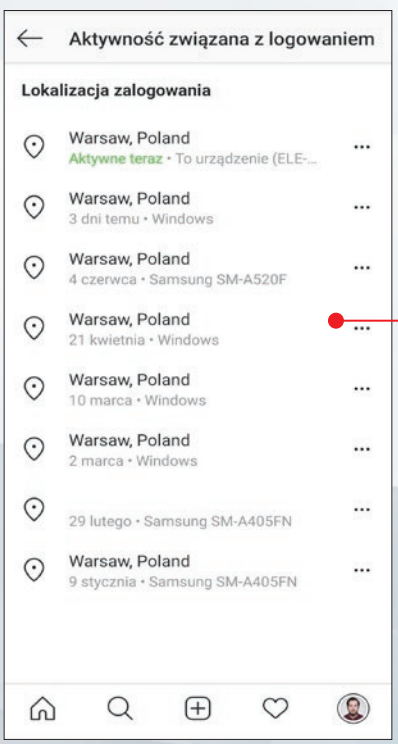


Instagram

Instagram to dla wielu osób nie tylko platforma do dzielenia się fotkami z wakacji, ale i narzędzie influencera i sposób na zarobek. Warto więc odpowiednio pilnować do niego dostępu. W aplikacji Instagram musimy najpierw rozwinąć menu, klikając na ikonę trzech kresek u góry ekranu. Na pojawiającej się liście wybieramy **Ustawienia** u dołu ekranu. W następnych krokach wybieramy **Zabezpieczenia** i **Aktywność dotycząca logowania**.



Tutaj możemy podejrzeć wszystkie urządzenia i miejsca, gdzie byliśmy zalogowani naszym instagramowym kontem. Kliknięcie na trzy kropki po prawej stronie otworzy szczegółowy widok z możliwością wylogowania się z konkretnego urządzenia.



JAK SOLIDNIE ZABEZPIECZYĆ SWOJE KONTA W INTERNECIE?

Włamania na konta w serwisach społecznościowych, pocztowych czy na platformach do grania to niestety smutna rzeczywistość. ***Programiści*** *pracujący nad rozwojem tych usług* ***dają nam jednak coraz więcej narzędzi do tego, by możliwie skutecznie zabezpieczać nasze wrażliwe i cenne dane na wiele sposobów****. Gdy bowiem zawiedzie jeden, nasze konto wciąż pozostanie nasze*

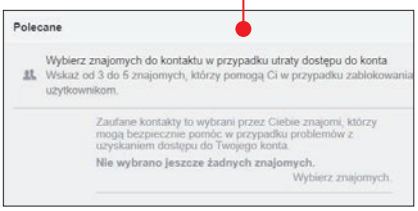
Facebook

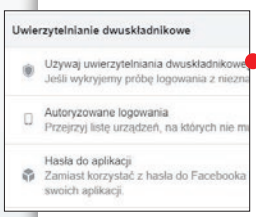
Zarządzanie zabezpieczeniami Facebooka dostępne jest z poziomu menu **Bezpieczeństwo i logowanie**. Aby tam dojść, w prawym górnym rogu głównego okna rozwijamy menu i wybieramy **Ustawienia i prywatność**, a następnie **Ustawienia**. W przypadku wersji smartfonowej konieczne będzie naciśnięcie przycisku menu (trzy kreski w prawym górnym rogu), a następnie przewinięcie okna w dół, do pokazania się funkcji **Ustawienia i prywatność**.

Zakładkę **Bezpieczeństwo i logowanie** znajdziemy po lewej stronie na górze okna lub w środkowej części okna w aplikacji mobilnej.

Tam znajdziemy trzy możliwości dodatkowego zabezpieczenia naszego konta.

Tu także możemy wybrać od trzech do pięciu kontaktów spośród najbardziej zaufanych znajomych. W momencie gdy stracimy dostęp do naszego konta, będą oni mogli pomóc nam je odzyskać.





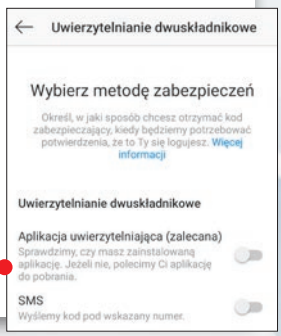
Uwierzytelnianie dwuskładnikowe, czyli logowanie dwustopniowe – gdy Face book wykryje logowanie na nasze konto z nowego, nieznanego urządzenia, poprosi o wpisanie kodu, który może być wysłany w wiadomości SMS na przypisany do naszego konta numer. W ten sposób nie tylko zabezpieczymy konto przed włamaniem, ale dowiemy się o ich próbach.

Jeżeli nie chcemy używać kodów, ale zależy nam na powiadomieniach o logowaniu, pomocna będzie funkcja **Otrzymuj powiadomienia o nierozpoznanych logowaniach**.

Instagram

Instagram umożliwia nam ustawienie uwierzytelniania dwuskładnikowego. Funkcję tę znajdziemy w panelu **Zabezpieczenia**. Rozwijamy menu z poziomu naszego profilu, klikając na ikonę trzech kresek u góry ekranu. Wybieramy **Ustawienia** u dołu ekranu. W następnych krokach wybieramy **Zabezpieczenia** i **Uwierzytelnianie dwuskładnikowe**.

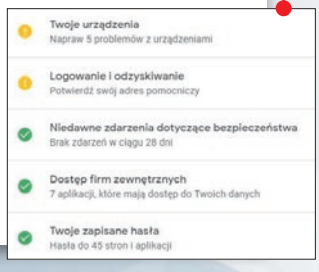
Po kliknięciu na przycisk **Rozpocznij** będziemy mogli wybrać, czy do potwierdzania logowania chcemy wykorzystać aplikację uwierzytelniającą, czy też kody SMS.



Gmail

W oknie dowolnego serwisu Google klikamy na ikonę naszego profilu i wybieramy **Zarządzaj kontem Google**.

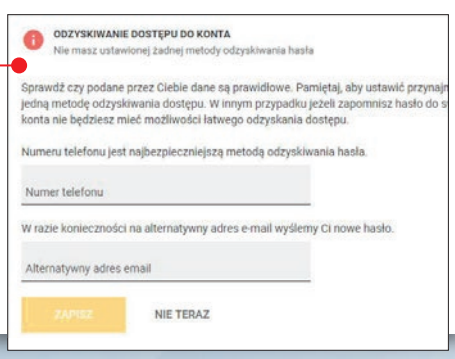
W nowo otwartym oknie znajdujemy zakładkę **Bezpieczeństwo**, a następnie w środkowej części znajdujemy przycisk **Zabezpiecz konto**. Zostaniemy przeniesieni do panelu sprawdzania zabezpieczeń, gdzie wykonując kolejne kroki, poprawimy bezpieczeństwo naszego konta poprzez na przykład dodanie adresów pomocniczych, na które wysłane zostaną informacje, gdy utracimy dostęp do naszego konta bądź zapomnimy danych logowania.



Onet Poczta

W przypadku klienta pocztowego Onetu, dla poprawy bezpieczeństwa konieczne jest zajrzenie do ustawień **O!Konta**. Do panelu ustawień dojdziemy, rozwijając menu w prawym górnym rogu i wybierając **Ustawienia konta**. Po lewej stronie przechodzimy do zakładki **Kontrola bezpieczeństwa**.

W głównym oknie możemy teraz wykonać kilka czynności związanych z bezpieczeństwem naszego konta. Zacznijmy od ustawienia numeru telefonu i alternatywnego adresu e-mail do odzyskiwania hasła w oknie **Odzyskiwanie dostępu do konta**. Następnie możemy ustawić weryfikację dwustopniową, która wymagać będzie podawania kodów przy logowaniu na nowych urządzeniach.



SILNE HASŁO TO PODSTAWA

Myśląc o zabezpieczeniach naszych kont, nie możemy zapomnieć o ustawieniu silnego hasła. Oznacza to hasło nieoczywiste, trudne do złamania, ale także odgadnięcia. Oto pięć najważniejszych zasad w tym aspekcie:

- Hasło powinno być unikatowe. Dla różnych serwisów zmieniaj chociażby kilka znaków lub cyfr,
- Hasło powinno składać się co najmniej z ośmiu znaków, w tym dużych i małych liter, cyfr i znaków specjalnych (na przykład !, $, *, @ itp.),
- Nie używaj prostych ciągów znaków (jak „1234” lub „qwerty”) ani także swojego imienia, nazwiska czy daty urodzenia,
- Hasło powinno być skonstruowane tak, byś mógł wpisać je szybko, korzystając ze znaków rozrzuconych na całej klawiaturze – zmniejszy to ryzyko podejrzenia hasła przez osoby postronne,
- Jeżeli nie wiesz, jakie hasło stworzyć, możesz skorzystać z generatorów haseł – łatwo znajdziesz je w sieci.

JAK ODZYSKAĆ SKRADZIONE KONTO?

Jeśli ktoś przejmie nasze konto w serwisie internetowym, nie wszystko stracone. Komputer Świat prezentuje ***procedury odzyskiwania konta w popularnych usługach***

Facebook

1 Jeśli nie możesz zalogować się na konto i podejrzewasz włamanie, udaj się na stronę **facebook.com/hacked**. Tutaj rozpoczniesz procedurę zgłaszania i odzyskiwania konta. Pod tym samym adresem możemy (jeśli jesteśmy zalogowani) zgłaszać nietypowe rzeczy pojawiające się na naszym koncie.

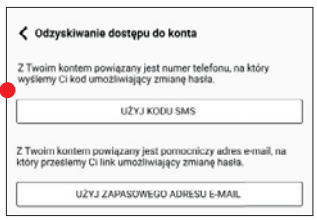
2 Wpisz adres e-mail lub numer telefonu skojarzony z twoim kontem. Jeśli nie pamiętasz tych danych, odzyskanie konta nie będzie możliwe.

3 Następnie wpisz ostatnio używane przez ciebie hasło. Jeśli faktycznie z niego korzystałeś, rozpocznie się procedura resetowania hasła. Na twój adres e-mail przyjdzie specjalny kod – wpisz go w odpowiednim polu.

4 Po zmianie hasła nastąpi dalszy ciąg procedury. Teraz możesz sprawdzić, jakie adresy e-mail są skojarzone z twoim kontem. Jeśli któreś nie należy do ciebie, możesz je usunąć.

5 Dla bezpieczeństwa wyloguj się z wszystkich urządzeń. Możesz to zrobić, wchodząc w **Ustawienia**, **Bezpieczeństwo i logowanie**, **Miejsce logowania**, **Wyloguj z wszystkich sesji**.

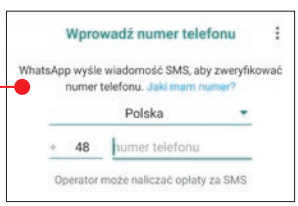
Onet Poczta



1 Na Onet Poczta możesz odzyskać hasło, korzystając z kodu SMS lub klikając na link wysłany na zapasowy adres e-mail. Przejdź przez kolejne kroki, wpisując w odpowiednie pola otrzymane dane. Jeśli będą się zgadzać, od razu otrzymasz dostęp do konta.

2 Jeżeli nie masz przypisanego zapasowego adresu e-mail lub numeru telefonu, konieczne będzie napisanie wniosku wraz z dołączoną fotokopią dokumentu tożsamości (z zasłoniętym numerem i serią dokumentu, numerem PESEL oraz zdjęciem właściciela). Sporządzony dokument wysyłamy na **profiling@grupaonet.pl**, a gotowy formularz znajdziemy na stronie Onet Poczty. (**https://pomoc.poczta.onet.pl/baza-wiedzy/formularz-wymuszenia-zmiany-hasla/**).

WhatsApp



1 Do WhatsAppa logujemy się naszym numerem telefonu. Jeśli haker ma dostęp do naszego konta, to znaczy, że w jakiś sposób otrzymał hasło SMS. Możemy go wylogować.

2 W tym celu reinstalujemy aplikację WhatsApp i logujemy się naszym numerem telefonu. Podajemy nowy kod SMS, a osoba korzystająca z naszego konta zostanie wylogowana.

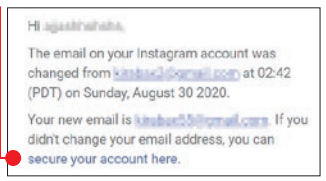
3 Jeśli oszust włączył weryfikację dwuetapową, musisz odczekać 7 dni, zanim możliwe będzie zalogowanie wyłącznie z użyciem kodu SMS. Chyba że podałeś adres e-mail do wyłączenia uwierzytelniania dwuskładnikowego – wtedy odzyskasz konto od razu.

Instagram

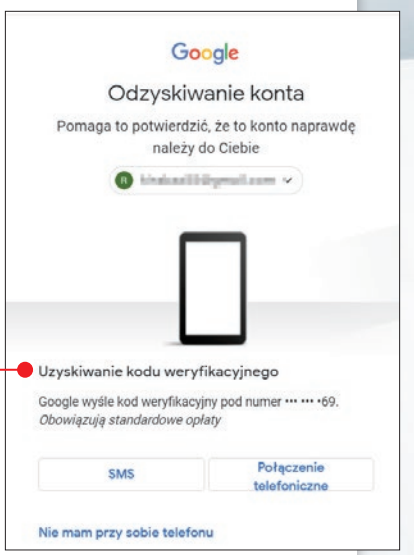
1 Na ekranie logowania klikamy na **Uzyskaj pomoc dotyczącą logowania się** i wpisujemy swój adres e-mail. Jeżeli go nie pamiętasz, niestety nie odzyskasz konta.

2 Jeśli jesteś pewien co do wpisanego e-maila, być może złodziej go zmienił. Wejdź na swoją skrzynkę i odszukaj wiadomości od Instagrama o treści **Email changed on Instagram**. Tam klikamy na **Secure your account here**.

3 W nowym oknie dostajemy podgląd na wpisane dane. Zabezpieczamy konto, resetując hasło. Stary adres e-mail zostanie przywrócony, a hasło zmienione.



Gmail



1 Aby odzyskać konto Google, musisz przypomnieć sobie wybrane dane podawane przy rejestracji – imię i nazwisko, e-mail pomocniczy lub odpowiedzi na pytania zabezpieczające.

2 Po wpisaniu adresu e-mail kliknij na **Nie pamiętam hasła**. Wpisz ostatnie zapamiętane przez ciebie hasło. Następnie na pomocniczy numer telefonu zostanie wysłany kod do resetowania hasła.

3 Jeśli nie masz przy sobie telefonu, w ciągu 6 godzin na pomocniczy adres e-mail otrzymasz formularz odzyskiwania konta. Najlepiej będzie, jeśli wypełnisz go ze skojarzonego urządzenia – smartfona czy komputera – a także domyślnej przeglądarki. Może być konieczne odpowiedzenie na pytania zabezpieczające. Poprawne wypełnienie przyspieszy odzyskiwanie konta.

4 Jeśli nie pamiętasz adresu e-mail, kliknij na **Nie pamiętasz adresu?**. W nowym polu wpisz numer telefonu lub e-mail skojarzony z odzyskiwanym kontem. Jeśli ich nie pamiętasz, na tym etapie odzyskanie konta nie będzie możliwe.

CZY MOJE HASŁO WYCIEKŁO DO SIECI?

Konta zakładamy w wielu serwisach i czasem może się zdarzyć z nich wyciek danych. Jeśli chcemy sprawdzić, czy nasz adres e-mail lub hasło zostały ujawnione w sieci, skorzystajmy ze strony **haveibeenpwned.com**. To bezpieczny serwis z ogromną bazą danych loginów i haseł, które wyciekły. Po wpisaniu naszego adresu e-mail pokazuje nawet, z których baz wydostał się na zewnątrz. Klikając zaś na górnym pasku na **Passwords**, możemy sprawdzić, czy nasze hasło należy do niebezpiecznych. Jeśli tak, strona poinformuje nas, ile razy wydostało się do sieci.

JAK REAGOWAĆ NA HEJT W SERWISACH SPOŁECZNOŚCIOWYCH?

Hejt, czyli mowa nienawiści, jest jednym z największych problemów w sieci i może doprowadzić do niebezpiecznych konsekwencji. ***Warto wiedzieć, jak reagować na tego typu zaczepki i jak je zgłaszać do administracji serwisu***

Przede wszystkim – zachować spokój i nie dać się sprowokować. Hejt w sieci jest bardzo często narzędziem tak zwanych trolli – osób, które „trollują", a więc specjalnie chcą wywołać kłótnię w sieci. Robią to całkowicie dla swojej rozrywki i zabawy, zwykle na przekór udając w rozmowie osobę o dokładnie przeciwnym nam nastawieniu. W takim wypadku najlepiej dyskusję zignorować.

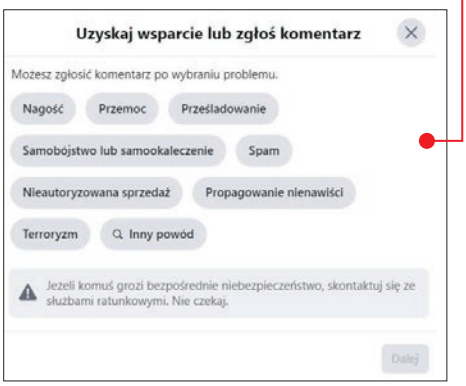
Są jednak przypadki prawdziwego hejtu, gdy ktoś jawnie nas albo bliskie nam osoby obraża i wyzywa. W tym wypadku także musimy pozostać spokojni i możliwie rzeczowi. W zależności od tego, czego dotyczy rozmowa, powinniśmy przede wszystkim skupiać się na konkretach. Rzeczowe i składne wypowiedzi są często doceniane przez innych użytkowników sieci, nawet w zalewie niewnoszącego nic hejtu.

A co w przypadku, gdy ktoś zwyczajnie chce nas urazić? Wtedy mamy możliwość zgłoszenia takiej wiadomości do administracji danego serwisu społecznościowego. W skrajnych przypadkach zalecamy także kierowanie sprawy na policję. Coraz rzadziej przypadki internetowych hejterów są bagatelizowane.

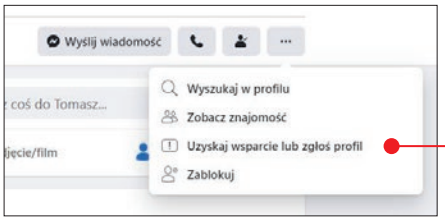
Jak wygląda proces zgłaszania hejterskiej wiadomości? Zaprezentujemy to na przykładzie dwóch popularnych serwisów, gdzie mowy nienawiści nie brakuje – Facebooka i Twittera.

Facebook

Jeżeli uznaliśmy, że ktoś rzeczywiście nas obraża, to mamy dwie możliwości. W przypadku komentarzy na przykład pod naszym postem możemy je ukryć, usunąć lub zgłosić. Opcje dostępne są po kliknięciu na trzy kropki obok samego komentarza – usunięcie pojawia się dopiero po ukryciu wpisu.



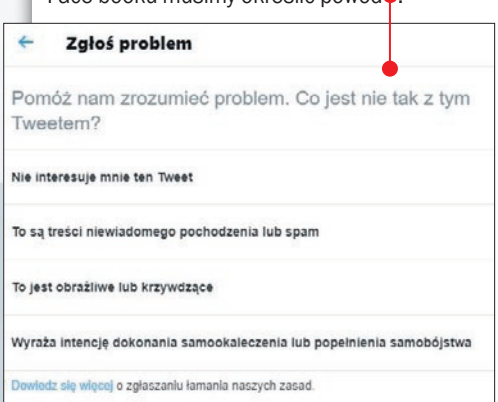
Po wybraniu opcji zgłoszenia musimy podać jego powód w nowym oknie. Niektóre opcje, jak na przykład **Propagowanie nienawiści**, rozwija się dalej, pozwalając zawęzić odbiór. Po zgłoszeniu komentarz lub post zostanie przesłany do moderacji, gdzie pracownik zdecyduje, czy rzeczywiście doszło do naruszenia regulaminu.



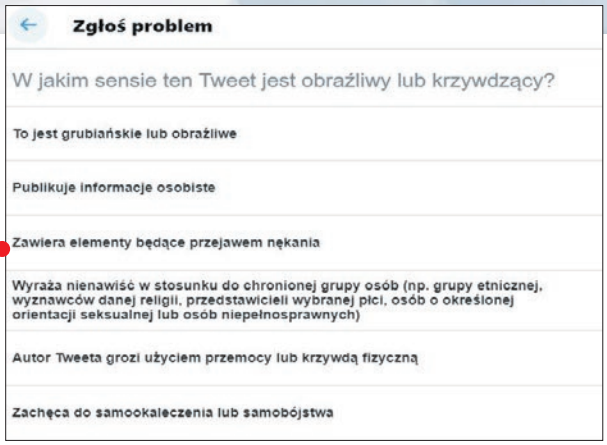
Facebook daje także możliwość zgłoszenia całego profilu. W tym celu należy wejść na profil danej osoby, wybrać z menu po prawej stronie opcję **Uzyskaj wsparcie lub zgłoś profil** i postępować analogicznie – wybrać powód i dokonać zgłoszenia.

Twitter

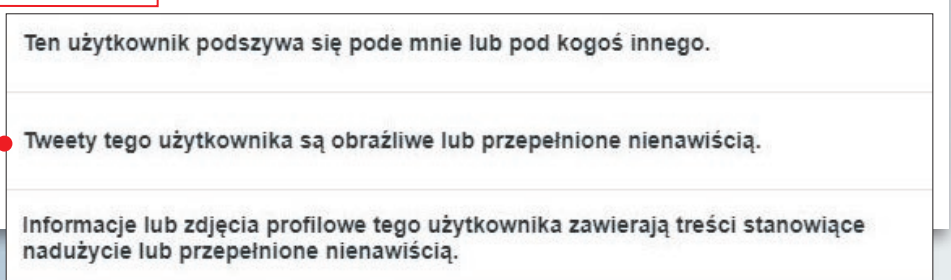
Na Twitterze także mamy możliwość zgłoszenia samej treści, jak i piszącej jej osoby. W tym pierwszym przypadku musimy rozwinąć menu wiadomości, którą chcemy zgłosić, a następnie wybrać opcję – **Zgłoś Tweeta**. Podobnie jak na Face booku musimy określić powód.



W przypadku hejtu będzie to opcja **To jest obraźliwe lub krzywdzące**. W dalszej części będziemy jeszcze proszeni o doprecyzowanie, o jaką formę obrazy lub krzywdzenia chodzi.

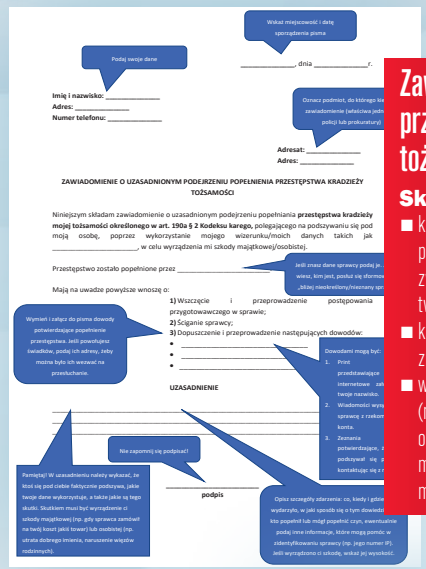


W przypadku zgłaszania profilu jest podobnie. Rozwijamy menu na stronie profilowej danej osoby i klikamy na **Zgłoś**. Interesująca nas kolejna opcja to **Tweety tego użytkownika są obraźliwe lub przepełnione nienawiścią**.



GOTOWE WZORY PISM

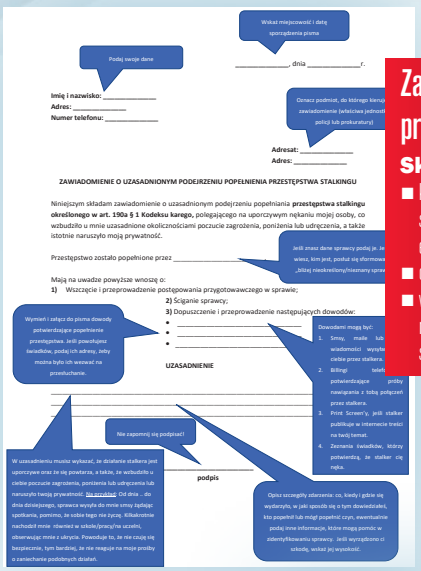
Zgłoszenie sprawy na policję lub do sądu wymaga przygotowania odpowiedniego wniosku. Prawnicy, autorzy tego Raportu Komputer Świata, przygotowali ***wzory, z których w razie potrzeby można skorzystać****. Pliki z dokumentami są do pobrania z KŚ Plus*



Zawiadomienie o popełnieniu przestępstwa kradzieży tożsamości

Skorzystaj z niego, gdy:

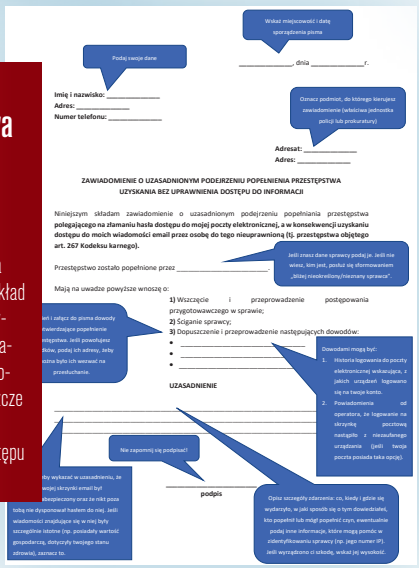
- ktoś bez twojej zgody założył konto na portalu społecznościowym na twoje nazwisko albo adres e-mail zawierający twoje dane;
- ktoś wysyła z nich wiadomości do twoich znajomych lub innych osób;
- wiadomości te są dla ciebie szkodliwe (na przykład stawiają cię w złym świetle, obrażają ich adresatów, powodują, że musisz zapłacić za coś, czego nie zamówiłeś)



Zawiadomienie o popełnieniu przestępstwa stalkingu

Skorzystaj z niego, gdy:

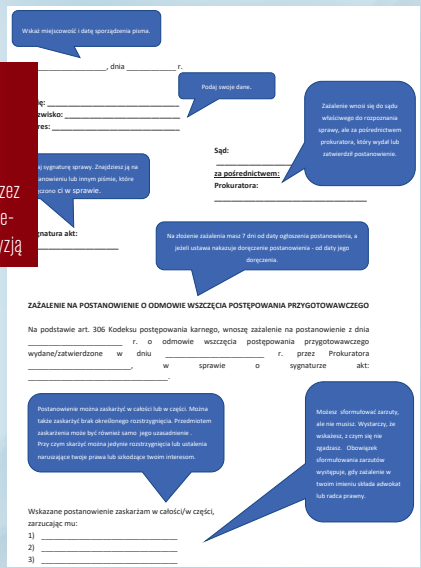
- ktoś od jakiegoś czasu cię nachodzi, śledzi lub wysyła do ciebie wiadomości e-mail, SMS etc.
- działania te są przez ciebie niechciane;
- wskutek tych działań czujesz się zagrożony, poniżony, udręczony lub istotnie naruszona została twoja prywatność



Zawiadomienie o popełnieniu przestępstwa nieuprawnionego dostępu do informacji

Skorzystaj z niego, gdy:

- zorientujesz się, że ktoś „wchodził" na twoją skrzynkę elektroniczną, na przykład otrzymałeś powiadomienie o nieuprawnionym logowaniu do twojego konta, zauważysz, że ktoś odczytał twoje wiadomości e-mail, pomimo że sam ich jeszcze nie czytałeś;
- zauważysz, że ktoś zmienił hasło dostępu do twojego konta



Zażalenie na odmowę wszczęcia postępowania

Skorzystaj z niego, gdy:

- prokurator nie uwzględnił złożonego przez ciebie zawiadomienia o popełnieniu przestępstwa i nie zgadzasz się z taką decyzją

Wzory pism w formacie .docx (Word) pobierzesz ze strony ksplus.pl. Niebieskie dymki zawierają przydatne informacje dotyczące wypełniania dokumentów – należy je wykasować, gdy już nie będą nam potrzebne.

Komputer Świat od 1998 roku

Adres redakcji: 02-672 Warszawa, ul. Domaniewska 49
internet: www.komputerswiat.pl, forum.komputerswiat.pl
e-mail: redakcja@komputerswiat.pl
Natalia Gaweł, Magdalena Kęska, Adam Książek, Kinga Rabęda, Klaudia Raczek, Rafał Rudnicki, Bartłomiej Sieja: autorzy tekstów
Rafał Kamiński: redaktor naczelny
Tomasz Paczuski: z-ca redaktora naczelnego, szef wydania drukowanego
Agnieszka Al-Jawahiri: z-ca redaktora naczelnego, szef wydań specjalnych
Jolanta Rososińska: korekta
Robert Dobrzyński: dyrektor artystyczny
Mariusz Rybak: redaktor graficzny

ringier axel springer

Wydawca: RINGIER AXEL SPRINGER POLSKA Sp. z o.o.
Członek Izby Wydawców Prasy i Związku Kontroli Dystrybucji Prasy
www.ringieraxelspringer.pl, asp@axelspringer.pl
Adres: 02-672 Warszawa, ul. Domaniewska 49
tel. 22 2320000, 22 2320001

Prezes Zarządu: Mark Dekan
Prezes Honorowy: Wiesław Podkański
Dyrektor Generalny: Marcin Biegluk
Dyrektor Wydawniczy: Paweł Paczuski
Dyrektor Finansowy: Krzysztof Stopa
Dyrektor Sprzedaży: Mariusz Wąsiński
Dyrektor Marketingu: Olga Korolec

media impact

Biuro reklamy: Media Impact
reklama.warszawa@mediaimpact.pl
tel. (12) 2600200 (BOK)

Business Project Manager: Paweł Bulwan
Dział personalny: Monika Remiszewska
Księgowość: Katarzyna Fita (dyrektor)
Kolportaż: Rafał Kamiński (dyrektor)
Produkcja: Mariusz Gajda
Druk: Walstead Kraków Sp. z o.o.

Prenumerata i egzemplarze archiwalne:
www.literia.pl

Zdjęcia na okładce:
iStockphoto.com

Sprzedaż internetowa: www.literia.pl
Prenumerata zagraniczna: www.literia.pl
E-wydania: ksplus.pl

Redakcja nie zwraca materiałów niezamówionych, zastrzega sobie prawo redagowania nadesłanych tekstów, nie odpowiada za treść zamieszczanych reklam i ogłoszeń

Zabroniona jest bezumowna sprzedaż czasopisma po cenie niższej od ceny detalicznej ustalonej przez wydawcę. Sprzedaż numerów aktualnych i archiwalnych po innej cenie jest nielegalna i grozi odpowiedzialnością karną.

Fot. Sinaappel/123rf.com, Nirut Punshiri/iStockphoto.com